

# Safety and Security Aspects of Software Assurance



**Warren Naylor, BAE Systems SETA II Support to:**  
**FAA, Office of Information Services**  
**Process Engineering Division, AIO-200**  
**Software Safety and Certification**  
**PH. (202) 548-5575**  
**[warren.naylor@baesystems.com](mailto:warren.naylor@baesystems.com)**

# FAA Mission Goals\*

## Safety and Security Aspects of Software Assurance

- Safety:
  - By 2007, reduce U.S. aviation accident rates by 80 percent from 1996 levels.
- Security:
  - Prevent security incidents in the aviation system
    - \*\*The FAA must ensure that all systems are protected from threats to integrity, availability, and confidentiality.

\* *FAA Achievement Plan: FAA Corporate Projects, FY 2000-2002 and Beyond*

\*\* *U.S. DOT/FAA Order 1370.82 (6/9/00)*

# Safety Strategies\*

## Safety and Security Aspects of Software Assurance

- Accident Prevention
- Safety Information Sharing and Analysis
- Certification and Surveillance

\* *FAA Achievement Plan: FAA Corporate Projects, FY 2000-2002 and Beyond*

# Information Security Strategies\*

## Safety and Security Aspects of Software Assurance

- Develop a systematic information security architecture that describes the future National Airspace System (NAS) information security system the FAA will build toward.

\* *FAA Achievement Plan: FAA Corporate Projects, FY 2000-2002 and Beyond*



# Safety and Security Definitions:

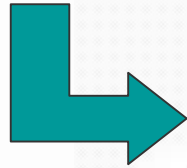
## Safety and Security Aspects of Software Assurance

- **Safety** is freedom from those conditions that can cause death, injury, occupational illness or damage to or loss of equipment or property or damage to the environment.
- **Security** is the prevention of advertent conditions that can cause death, injury, occupational illness or damage to or loss of equipment or property or damage to the environment.

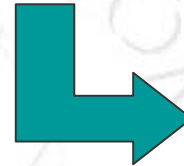
# Safety and Security Similarities

## Safety and Security Aspects of Software Assurance

### ANALYSIS



### REQUIREMENTS



### VERIFICATION

#### SECURITY

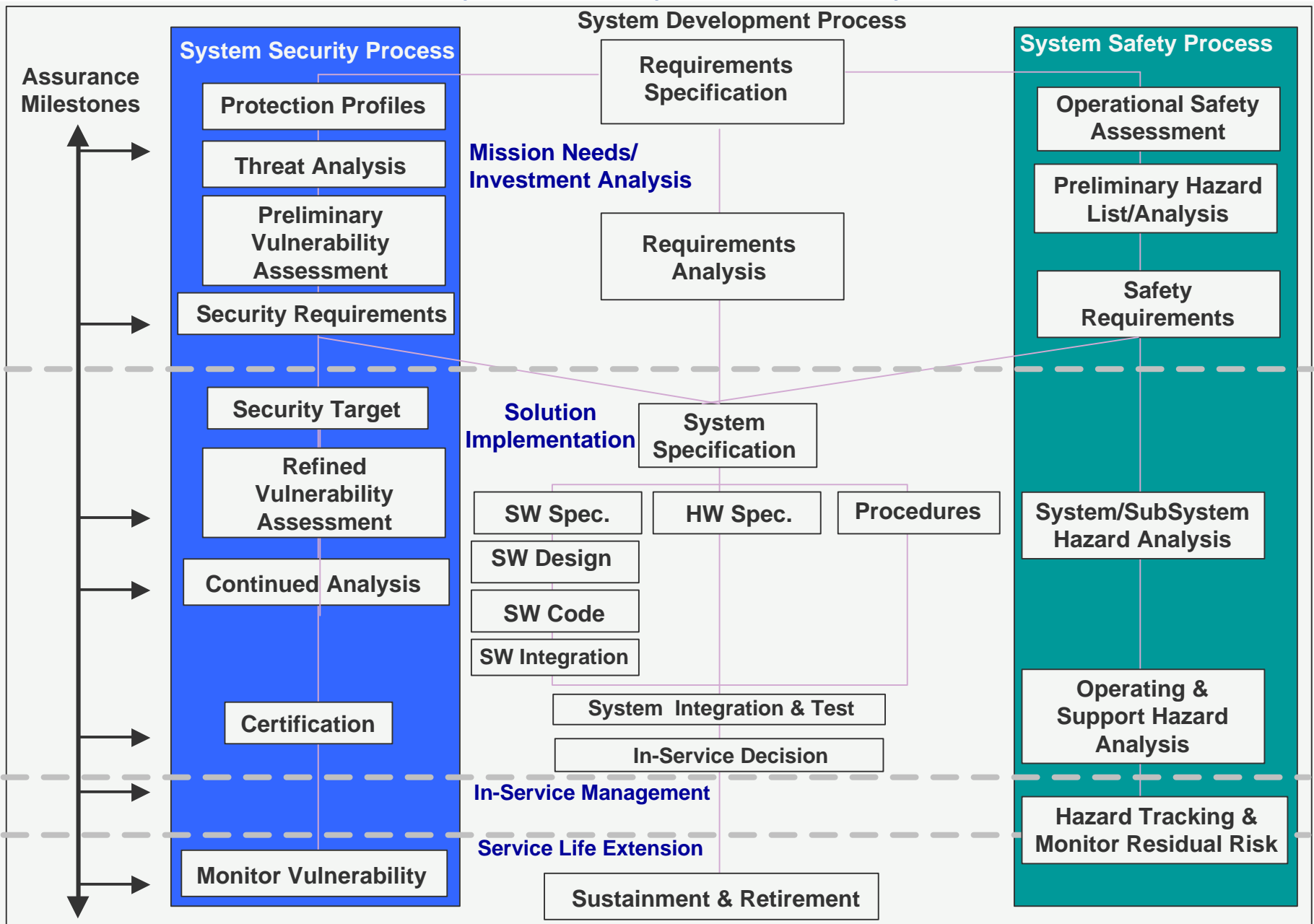
- Vulnerability/Threat Assessment
- Risk Determination
- Security Requirements
- Penetration testing



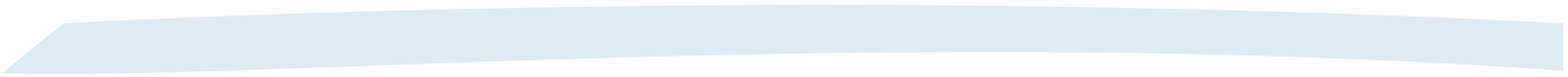
#### SAFETY

- Operational Safety Assessment
- Risk Determination
- Safety Requirements
- Requirements-based testing

# Preliminary Safety/Security Model



# FAA Safety Initiatives



\*The accident rate for commercial aviation declined dramatically between 1950 and 1970. But, over the last two decades, that rate has remained low, but flat. Heading into the next century, the overall goal of aviation safety programs is clear: to bring that rate down even lower. Focusing on the accident rate is critical because of the projected increases in traffic. Unless that rate is reduced, the actual number of accidents will grow as traffic increases. Given the international nature of aviation, cutting the accident rate is an imperative not just for the United States, but for all countries involved in aviation.

*\*White House Commission on Aviation Safety and Security FINAL REPORT TOPRESIDENT CLINTON*

# Safety Strategies\*

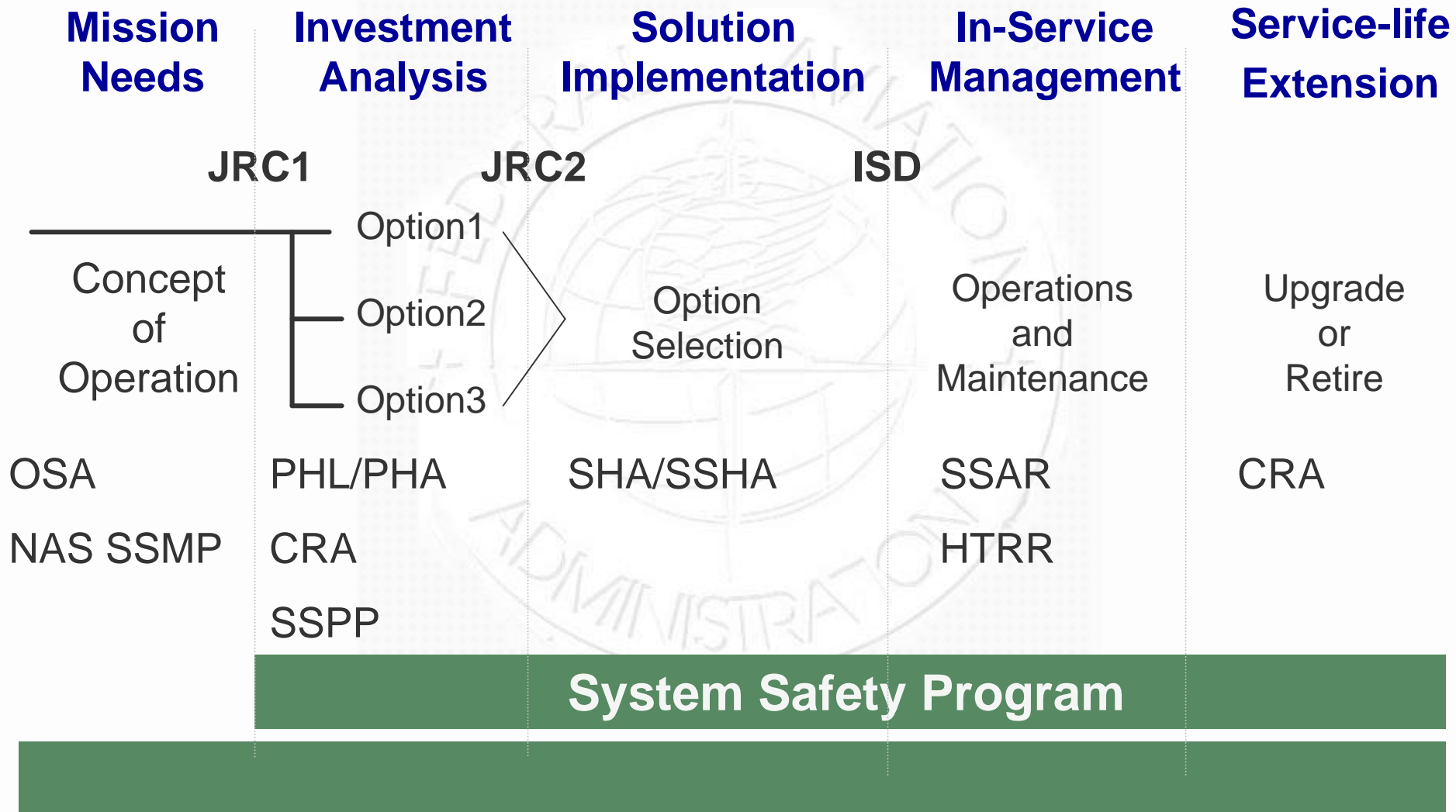
## Safety and Security Aspects of Software Assurance

- Accident Prevention
- Safety Information Sharing and Analysis
- Certification and Surveillance

\* *FAA Achievement Plan: FAA Corporate Projects, FY 2000-2002 and Beyond*

# System Safety Within the AMS Process

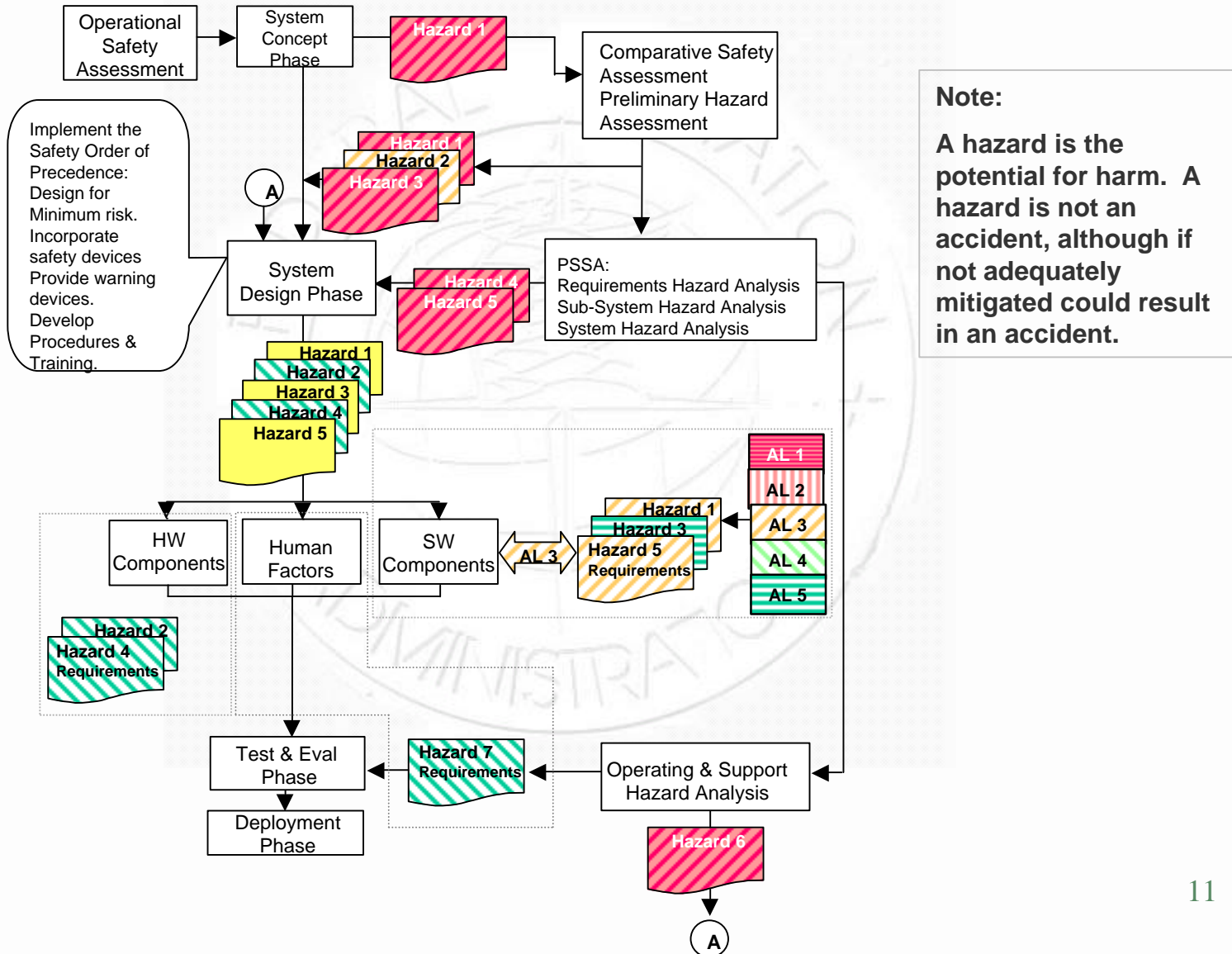
## Safety and Security Aspects of Software Assurance



Tracking)

# Simplified Iterative Safety Model

## Safety and Security Aspects of Software Assurance





# Universal Safety Order of Precedence

## Safety and Security Aspects of Software Assurance

- ✓ **Design for Minimum Risk.** The system design will seek to eliminate hazards. If an identified hazard cannot be eliminated, the associated risk will be reduced to an acceptable level through design selection.
- ✓ **Incorporate Safety Devices.** When identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk will be reduced to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices.
- ✓ **Provide Warning Devices.** Warning devices may be utilized to augment or reduce the probability of a hazard occurrence when neither design or safety devices effectively eliminate or reduce the associated risk to an acceptable level. Warning signals and their application shall be succinct and easily understood to reduce the risk of misinterpretation and shall be standardized to be consistent with other like systems.
- ✓ **Develop Procedures and Training.** When risk reduction is not adequately achieved through design, safety devices, and/or through warnings, then training and implementation of procedures and training are utilized.



# Human Factor Considerations

## Safety and Security Aspects of Software Assurance

- **The human is the single most important and unpredictable element in any system!** Therefore, the following factors must be considered in the design to ensure the safe and proper operation of the fielded system:
  - Training
  - Maintenance
  - Operational Environment
  - Visual Displays
  - Cognitive Workloads
  - Automated Features
  - Data Entry
  - Error Alerts
  - Keyboards & Control Devices

# System Engineering Council

## Safety and Security Aspects of Software Assurance


- Purpose
  - Orchestrates common systems engineering activities across the NAS
  - Responsibility, authority, and accountability for the development, documentation, deployment, control, and monitoring of the systems engineering process.
- Products
  - System Engineering Management Plan
  - System Engineering Manual

# System Safety Working Group

## Safety and Security Aspects of Software Assurance

- Purpose
  - Working arm of the System Engineering Council
  - Assists in supporting and evaluating Comparative and Operational Safety Assessments
- Products
  - System Safety Management Plan
  - System Safety Handbook

# FAA Security



\*The security of information systems and networks (is) the major security challenge of this decade and possibly the next century...there is insufficient awareness of the grave risks we face in this arena.

*\*Redefining Security, Joint Security Commission*

# Terrorism – A Real Threat !

## Safety and Security Aspects of Software Assurance

- The Internet is becoming a resource more frequently used by terrorists as a means to access information, spread propaganda, raise funds, communicate, and plan operations; and the possibility of a terrorist threat involving government and commercial computer-driven applications is a growing concern.

# Terrorism – A Real Threat !

## Safety and Security Aspects of Software Assurance

- Adequate security to protect against hacker-type inroads and cyberattacks remains a never-ending battle of technology.
- A concerted terrorist assault on computer networks could bring down communications and power grids in a manner reminiscent of the North American winter ice-storm of 1998, and could create havoc in the business community. Similarly, the physical destruction of critical computer networks could seriously cripple key global commercial infrastructures such as air transport, stock markets and exchanges, and international banking. ]

# Information Security Strategies\*

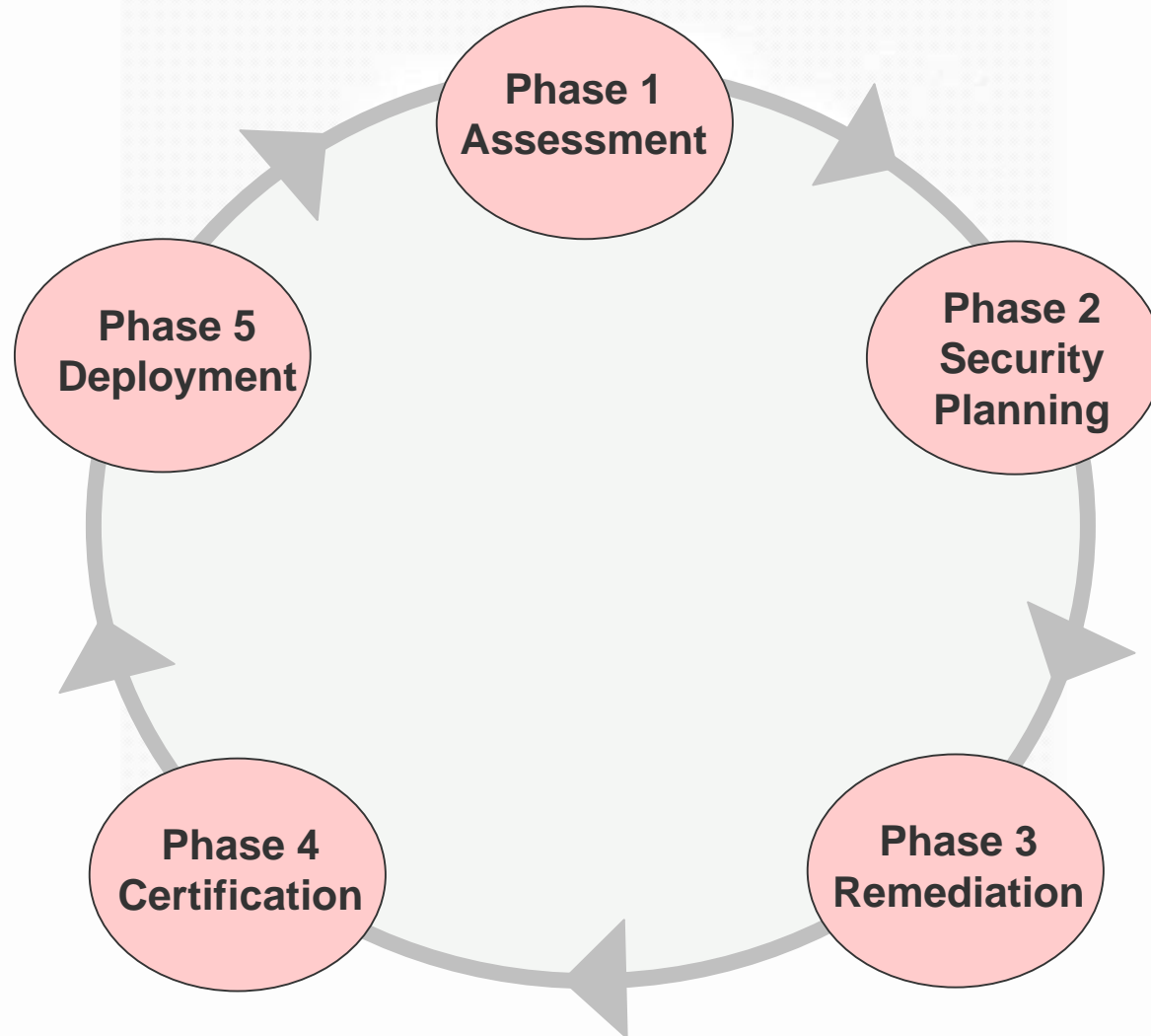
## Safety and Security Aspects of Software Assurance

- Develop a systematic information security architecture that describes the future National Airspace System (NAS) information security system FAA will build toward.

\* *FAA Achievement Plan: FAA Corporate Projects, FY 2000-2002 and Beyond*

# Simplified Iterative Security Model

## Safety and Security Aspects of Software Assurance

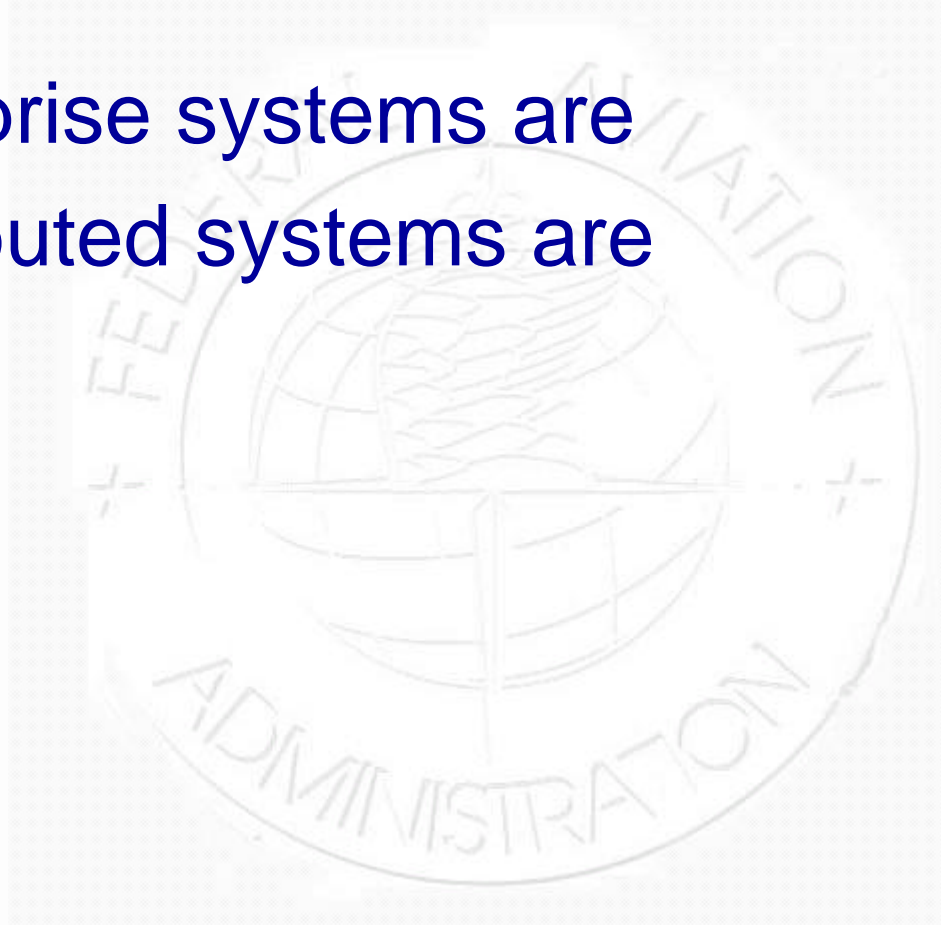




# Enterprise vs. Distributed Systems

## Safety and Security Aspects of Software Assurance

- Enterprise systems are
- Distributed systems are

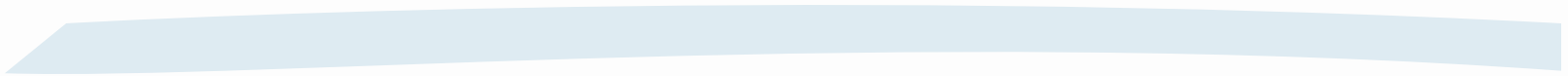


# Enterprise vs Distributed Vulnerabilities

## Safety and Security Aspects of Software Assurance

- **Enterprise systems are less vulnerable to intrusion and viruses:**
  - Only one firewall to maintain
  - Shared software
    - Utilities
    - File managers
    - Database management
    - Electronic Messaging
    - Access
    - Centralized applications
- **Enterprise systems are less vulnerable to intrusion and viruses:**
- **Distributed systems are more vulnerable to intrusion and viruses:**
  - Multiple firewalls to maintain

# FAA Software Assurance



# FAA CNS/ATM Software

## Safety and Security Aspects of Software Assurance

- FAA-iCMM
- Software development
- Software assurance

*Implement and integrate software engineering processes into systems engineering.*



# Software Quality Triangle

## Safety and Security Aspects of Software Assurance

Establishes a level of confidence for software that is consistent with its environment

**Software Assurance  
Guidance**

Establishes a process and documentation guidance for software development

**FAA-STD-026  
(IEEE12207)**

**QUALITY SW  
FOR NAS  
SYSTEMS**

**FAA-iCMM**

Establishes essential elements of an organizations software acquisition, engineering, and management process

# Software Assurance

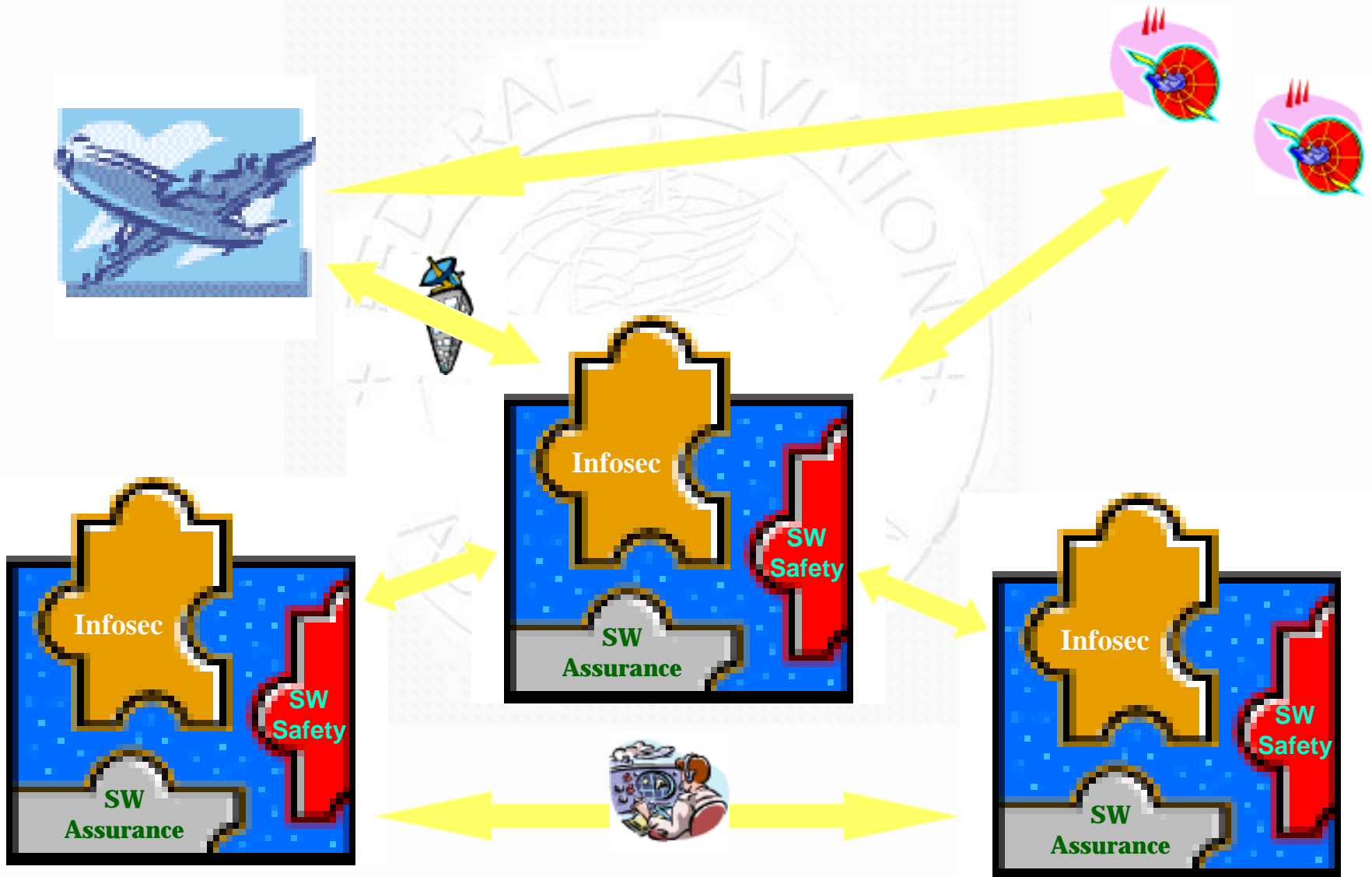
## Safety and Security Aspects of Software Assurance

- What do we want to achieve?

Identify the objectives necessary, throughout the life cycle process, to provide confidence that a product and process satisfies defined safety and security integrity level requirements. ICAO has established a targeted Global Risk Factor of extremely remote or  $10^{-7}$ .

# Compounding Complexities

## Safety and Security Aspects of Software Assurance



# Summary

## Safety and Security Aspects of Software Assurance

- The FAA continues to refine its systems and software engineering processes
- We are focusing on the technical and programmatic efficiencies that can be achieved by integrating safety and security into the system life cycle processes.



Backup slides



## Acronyms (1/2)

- AMS Acquisition Management System
- CRA Comparative Risk Analysis
- FAA Federal Aviation Administration
- FMEA Failure Modes Effects Analysis
- HTRR Hazard Tracking and Risk Resolution
- ICAO International Civil Aviation Organization
- ISD In-service Decision
- JRC Joint Resource Council
- LMS Life-cycle Management System
- NAS National Airspace System

# Acronyms (2/2)

## Safety and Security Aspects of Software Assurance

- OSA      Operational Safety Assessment
- PHA      Preliminary Hazard Assessment
- SEMP      System Engineering Management Plan
- SEM      System Engineering Manual
- SHA      System Hazard Analysis
- SSH      System Safety Handbook
- SSHA      SubSystem Hazard Analysis
- SSMP      System Safety Management Plan
- SSAR      System Safety Assessment Report